We've got a lot to learn from hackers

DIGITAL SURVIVOR

JIM CARROLL

When you think about the Internet and e-commerce security, you may have an image of a computer geek, hacking away in isolation, breaking into corporate sites through sheer brilliance.

Think again. While people have to be fairly smart to figure out how to break into an e-commerce or Web site, they don't a need stratospheric IQ. They can simply immerse themselves in the on-line hacker culture to learn about the latest security-cracking exploits.

If you are responsible for some type of on-line initiative, you need to understand how the majority of security risks happen.

For managers, it is doubly important to be aware. You are ultimately responsible for ensuring that the people involved with your e-commerce initiative are doing the right things to secure your site.

First, appreciate that a hacker culture exists on the Internet through which people readily share information on latest security holes or weaknesses in various computer programs or operating systems.

A tour of some of the more public of such sites — Rootshell (**www.rootshell.com**), Lopht (**www.lopht.com**) and Fyodor's Playhouse (**www.insecure.org**) — reveals but a small part of this hacking world.

While deeply technical, each of these sites is full of reports on the latest security problems found with Web server software, e-mail programs, e-commerce applications and operating systems.

Scan them and you'll quickly realize that huge numbers of new problems are found each week. Dig deeper and you'll even find some software that can help you hack.

In exploring these sites, keep in mind that there are two types of people in the community. Sites such as those above are built by true "hackers," people who like to explore the limits of computer systems merely for the joy of doing so.

But on the darker side of the Internet, you can find more impressive (and scary) information resources built by "crackers," those who find and exchange such information with the specific intent of doing something wrong.

Sites such as those listed here receive much of their information because many honourable hackers like to find out where "bad programming" or "lousy software design" has led to security risks. In this way, they are performing a useful community service, and we should appreciate them for what they do.

There is an element within the computer community that revels in pointing out the particular problems that exist in Microsoft software. A section within insecure.org, for example, features the headline "Hack the Evil Empire."

Many people take great delight in pointing out that while Microsoft is an industry leader, it doesn't generally have a good reputation within the technical community for building highly reliable or secure software.

You can expect that when Windows 2000 ships in the next month, there will be countless Web pages highlighting how to take advantage of the flaws within the platform — such is the joy brought to the community.

According to experience, most high-profile security problems have come about directly as a result of negligence. In a well-publicized case last year, for example, a man reported that he could access the full credit card details of at least 100 on-line stores.

Was he a genius? Probably not. He simply discovered that the people who implemented these e-commerce sites didn't follow a recommended set of instructions on how they should "lock down" access to a particular area.

In many cases, problems come about because people ignore the highly publicized security problems that have been identified by the hacker community.

As you roll out your e-commerce platform, make sure you pay enough attention to security issues. Assess the expertise of your technology partners to determine whether they are up to date with the hacker community, and continually monitor your platform. The best way to appreciate how involved you must become is to explore the hacker culture.

◆ ◆ ◆

Jim Carroll is co-author of Light Bulbs to Yottabits: How to Profit by Understanding the Internet of the Future, *and can be reached by E-mail at jcarroll@jimcarroll.com*